Status of the Claims:

Although the claims have not been amended, below is a listing of the claims as they now stand:

1. A method of preventing undesirable activities of Executable Objects via an application, comprising:

denying to the same application, or one or more of its threads, access to a secured resource if said application, or one or more of its threads, has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource; and

denying said application, or one or more of its threads, Internet behavior if, at a time access is sought to the Internet, said application, or one or more of its threads is accessing a secured resource.

2. A method according to claim 1, further comprising recording in a memory events representative of Internet behavior, keeping a record of all secured resources that are to be kept secured and when an application that has previously exhibited Internet behavior attempts to access one such secured resource, denying access to said secured resource, unless:

a) At least a predetermined period of time has passed since a last Internet behavior; or

b) Said application, or one or more of its threads, has performed at least a predetermined number of operations after exhibiting Internet behavior; or

c) Another preset condition has been fulfilled.

3. A method according to claim 2, wherein the preset condition comprises an exercise of control over execution of downloadables received during Internet behavior, to ensure that no unexecuted downloadable may access the secured resource.

4. A method according to claim 2, wherein the present condition comprises an analysis of downloadables to ascertain the downloadables are harmless.

5. A method according to claim 1, wherein Internet behavior is denied by disabling a network connection creation.

6. A method according to claim 1, wherein Internet behavior is denied by disabling specific protocols.

7. A method according to claim 6, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

8. A method according to claim 1, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

9. A method according to claim 5, wherein access to trusted sites is not denied.

10. A method according to claim 1, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

11. A method according to claim 1, wherein all sub-threads of a thread that is denied access to a secured resource are also denied access to secured resources.

12. A method according to claim 1, wherein all sub-threads of a thread that is denied Internet behavior are also denied Internet behavior.

13. An apparatus for preventing undesirable activities of Executable Objects via an application, comprising:

a memory for storing a record of Internet behavior of a plurality of applications; and

means for denying to an application access to a secured resource if the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

14. An apparatus for preventing undesirable activities of Executable Objects via an application, comprising:

a memory of storing a record of Internet behavior of a plurality of applications; and

means for denying an application, or one or more of its threads, Internet behavior if, at a time access is sought, said application, or one or more of its threads, is accessing a secured resource.

15. A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet, or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying to an application access to a secured resource if the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

16. A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying an application, or one or more of its threads, Internet behavior if, at a time Internet behavior is exhibited, said application, or one or more of its threads, is accessing a secured resource.

17. (Cancelled)

18. A method according to claim 2, wherein Internet behavior is denied by disabling a network connection creation.

19. A method according to claim 3, wherein Internet behavior is denied by disabling a network connection creation.

20. A method according to claim 4, wherein Internet behavior is denied by disabling a network connection creation.

21. A method according to claim 2, wherein Internet behavior is denied by disabling specific protocols.

22. A method according to claim 3, wherein Internet behavior is denied by disabling specific protocols.

23. A method according to claim 4, wherein Internet behavior is denied by disabling specific protocols.

24. A method according to claim 21 wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

25. A method according to claim 22, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

26. A method according to claim 23, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

27. A method according to claim 2, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

28. A method according to claim 3, wherein Internet behavior is denied by disabling transfer of executable objects in communication protocols.

29. A method according to claim 4, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

30. A method according to claim 1, wherein access to trusted sites is not denied.

31. A method according to claim 2, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

32. A method according to claim 3, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

33. A method according to claim 4, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.